河南省教育信息安全监测中心
关于通达 OA 存在任意文件下载漏洞的安全风险预警

河南省教育信息安全监测中心
Henan Provincial Education Information Security Monitoring Center

2023 年 12 月 28 日

关于通达 OA 存在任意文件下载漏洞的安全风险预警

事件描述

近期发生多起重要单位使用的北京通达信科科技有限公司网络智能办公系统(OA)存在任意文件下载漏洞的事件。经初步分析，由于该系统(低于 11.09 版本)的接口“down.php”未过滤用户传入的参数，导致攻击者可跨越目录，从而实现任意文件下载。

漏洞编号

暂无

受影响版本

通达 OA < 11.09 版本

漏洞 POC

http(s):/XXXX/inc/package/down.php?id=../../../cache/org

修复方案

厂商已发布升级补丁，请升级至安全版本及以上，以

修复该漏洞。

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893、0371-67765016

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052